УДК 681.3.06

О НЕКОРРЕКТНОСТИ СТАНДАРТНОГО УСЛОВИЯ ДЛЯ MOV-АТАКИ НА ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

А.В. БЕССАЛОВ

Дан анализ двух условий для бидинейного спаривания точек и MOV- атаки, определенных теоремой Кассельса. Замечено, что стандартное условие для MOV- атаки отвечает лишь одному из условий теоремы Кассельса и не гарантирует возникновение нециклической структуры группы точек. Предложено в будущих стандартах добавить к тесту проверку наличия квадрата в порядке кривой.

Ключевые слова: эллиптические кривые, кривые Эдвардса, порядок кривой, порядок точки, простое поле, расширенное поле.

ВВЕДЕНИЕ

Широко известная в сфере криптографии работа [1] предложила одну из первых атак изоморфизма на проблему дискретного логарифмирования (DLP) в группе точек эллиптической кривой. Эта атака, получившая по именам авторов название MOV-атаки, сводится к отображению пары точек кривой E над некоторым расширением F_q^k поля F_q в элемент поля расширения, что при небольших значениях k катастрофически снижает сложность DLP. Из большинства криптоприложений после этой работы были исключены уязвимые к MOV-атаке суперсингулярные кривые, а все появившиеся через десятилетие стандарты (в частности, [2–7]) включили обязательные тесты на стойкость кривой к MOV-атаке. Автор данной статьи обнаружил, что результат тестирования и действительная уязвимость кривой к MOV-атаке могут оказаться далекими друг от друга, в итоге отбраковываются достаточно стойкие кривые, но не выдержавшие тест. В статье для убедительности приводится простой пример, иллюстрирующий вышесказанное.

УСЛОВИЯ ДЛЯ MOV-АТАКИ И УСЛОВИЯ ТЕСТИРОВАНИЯ В СТАНДАРТАХ

Пусть $N_E = hn$ – порядок кривой E над конечным полем F_q, где n – большое простое число, а кофактор h невелик (обычно $h \le 4$). Криптосистема строится на циклической подгруппе точек кривой простого порядка n.

Изоморфное отображение, рассмотренное в [1], строится как билинейное спаривание Вейля (или Тейта и др.) двух точек кривой в расширении F_q^k, $k = 1, 2, 3,...$, в котором возникает нециклическая группа $nG \times nG$ точек порядка n, содержащая n^2 точек. Спаривание необходимым образом использует две точки из разных циклических подгрупп порядка n нециклической группы порядка n^2 [9]. Можно, таким образом, утверждать, что достаточным условием для MOV-атаки является возникновение нециклической группы точек порядка n в некотором расширении поля F_q. В принципе нециклическая группа точек может существовать и в поле F_q ($k = 1$), если $h = cn$, но это не отвечает принятым ограничениям. Для суперсингулярных кривых нециклическая группа образуется уже при $k = 2..6$, для несуперсингулярных – значения k, как правило, достаточно велики и могут оказаться соизмеримыми с порядком поля q. В исключительных случаях группа $nG \times nG$ может возникнуть и при небольших значений k, что и требует MOV-тестирования всех, в том числе и несуперсингулярных кривых.

Необходимые условия для нециклической структуры группы E_q формулируются в теореме Кассельса [8, с.85]: группа E_q порядка $N_E = n_1 n_2$ является либо циклической, либо представляется прямой суммой двух циклических подгрупп порядков n_1 и n_2, таких что

$$n_1 \mid n_2 \text{ и } n_1 \mid \text{НОД}(N_E, q-1) \qquad (1)$$

Отсюда, в частности, следует, что порядок N_E содержит квадрат n_1^2. Заметим, что выполнение обоих условий (1) еще не гарантирует нециклической структуры группы (хотя, как правило, это так). Многие циклические кривые, например, содержат квадраты в порядке кривой [8]. Необходимые и достаточные условия нециклической структуры эллиптической кривой для общего случая пока не определены.

Обратимся теперь к известным стандартам [2-7]. Тест на стойкость кривых к MOV-атаке в них состоит в проверке неделимости $n \nmid q^k - 1$ для всех $k = 1..B$, с возможно различными значениями верхней границы B. Этот тест, отвечающий лишь второму условию (1) теоремы Кассельса, даже не гарантирует квадрата n^2 в порядке кривой в расширении F_q^k. Его можно было бы классифицировать как «подозрение на уязвимость к MOV-атаке». Конечно, это не снижает безопасности проектируемых криптосистем, однако вряд ли обоснованным (и корректным) является упрощенный тест, отвергающий приемлемые для криптосистем кривые. По-видимому, более целесообразно при доработке стандартов усилить этот тест по меньшей мере дополнительной проверкой на наличие квадрата n^2 в порядке кривой над большим полем.

Пример. Для иллюстрации примем порядок точки $n = 3$ и построим несуперсингулярную кривую

$$y^2 + xy = x^3 + ax^2 + b, \; b \ne 0 \qquad (2)$$

над полем F_2^2 ($q = 2^2$) с неприводимым полиномом $P(x) = x^2 + x + 1$ и его корнем α, для которого $\alpha^2 + \alpha + 1 = 0$. Здесь α – генератор мультипликативной

группы поля F_2^2 3-го порядка ($\alpha^3 = 1$) со следом 1. В границах Хассе 2..8 с четными значениями N_E нас устраивает лишь кривая с порядком $N_E = 6 \equiv 2 mod 4$, поэтому коэффициент a в (2) должен иметь след 1[8]. Примем $a = \alpha$. Для точки $Q = (x_1, y_1)$ 3-го порядка $2Q = -Q$ нетрудно получить уравнение

$$x_1^4 + x_1^3 + b = 0, \qquad (3)$$

которое в нашем случае ($x_1^3 = 1$) принимает вид $x_1 = 1 + b$. Значения $b \neq 0, 1$ (в последнем случае получим точку 2-го порядка), поэтому примем $b = \alpha$, тогда кривая $y^2 + xy = x^3 + \alpha x^2 + \alpha$ имеет точки 3-го порядка $Q = (\alpha^2, \alpha^2)$, $-Q = (\alpha^2, 0)$, а порядок кривой $N_E = 6$. Так как $N_E = q + 1 - t_1$, то параметр t_1 (след уравнения Фробениуса) равен $t_1 = -1$.

Найдем порядки этой кривой над над расширениями $F_q^2 = F_2^4$ и $F_q^3 = F_2^6$. Рекуррентная формула расчета параметра t_k имеет вид [8]

$$t_{k+2} = t_1 t_{k+1} - q t_k, \quad k = 0, 1, 2, \ldots, \ t_0 = 2.$$

Отсюда $t_2 = -7$, $N_{E2} = q^2 + 1 - t_2 = 24$, $t_3 = 11$, $N_{E3} = q^3 + 1 - t_3 = 54$. Хотя в этом примере $n|(q-1)$ и $n|(q^2-1)$, о билинейном спаривании (или MOV-атаке) речи не идет, поскольку порядки соответствующих кривых 6 и 24 не делятся на 3^2. И только расширение степени $k = 3$ с выполнением $n|(q^3 - 1)$ дает нециклическую группу типа (2, 3, 3^2), имеющую ровно 3^2 точек порядка 3. Порядок кривой $N_{E3} = 54 = 2 \cdot 3^3$ содержит квадрат 3^2 и выполняются оба условия теоремы Кассельса (1). Кроме того, кривая действительно содержит 9 точек 3-го порядка (что и является условием нециклической группы точек 3-го порядка). Действительно, уравнение (3)

$$x_1^4 + x_1^3 + \beta^{21} = 0, \qquad (4)$$

в поле F_2^6 с примитивным элементом β, для которого $\beta^6 + \beta + 1 = 0$, имеет ровно 4 решения. В уравнении (4) $\beta^{21} = \alpha$ – элемент подполя F_2^2 3-го порядка. Одно из решений (4) лежит в этом подполе и является тривиальным $x_1^{(1)} = \alpha^2 = \beta^{42}$. Остальные 3 решения принадлежат расширению F_2^6 и равны

$$x_1^{(2)} = \beta^{23} = 101001, \quad x_1^{(3)} = \beta^{29} = 111000,$$
$$x_1^{(4)} = \beta^{53} = 101010.$$

Каждое из решений (4) дает по 2 точки 3-го порядка, в итоге вместе с точкой на бесконечности имеем 9 точек 3-го порядка и, следовательно, нециклическую структуру группы.

Итак, хотя тест на MOV-атаку в примере отбраковывает все кривые с расширениями степени $k = 1, 2, 3$, уязвимой к MOV-атаке является лишь кривая над полем F_q^3.

В заключение еще раз подчеркнем, что стандартный тест на MOV-атаку стал бы более корректным, если его усилить дополнительной проверкой: $n^2 \nmid N_{Ek}$, где N_{Ek} – порядок кривой E в расширении F_q^k.

Литература

[1] *Menezes A.J, Okamoto T., Vanstone S. A.* Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. University of Waterloo, sep. 1990. And //IEEE Transactions on Information Theory, V39, 1993. – PP 1639-1646.

[2] *IEEE P1363-2000.* Standard Specifications for Public Key Cryptography. Institute of Electrical and Electronics Engineers, Inc.,2000.

[3] *ISO/IEC JTC* 1/SC 27 n 2303, CD 15946-2. Information Technology- Sequrity Techniques – Cryptographic Techniques based on Elliptic Curves: Part 2- Digital Signatures. 1999 -05-26..

[4] *ANSI X9.62-1999.* Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). 1999.

[5] *FIPS 186-2.* Digital Signature Standard. National Institute of Standard and Technology. 2000.

[6] *ГОСТ Р 34.10-2001.* Информационная технология. Криптографическая защита информации. Процедуры формирования и проверки электронной цифровой подписи. – М.: Госстандарт России, 2001. – 20с.

[7] *Державний стандарт України ДСТУ 4145-2002.* Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння. Київ, Держстандарт України, 2003. – 94с.

[8] *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых: Учеб. Пособие. – К.: ІВЦ «Видавництво «Політехніка»», 2004, 224 с.

[9] *Markus Jakobsson and Wenbo Mao.* Cryptographic Protocols. Prentice-Hall, 2006.

Поступила в редколлегию 5.04.2012

Бессалов Анатолий Владимирович, фото и сведения об авторе см. на с. 226.

УДК 681.3.06

Про некоректність стандартної умови для MOV-атаки на еліптичні криві / А.В. Бессалов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 238–239.

Дано аналіз двох умов для білінійного спарювання точок і MOV- атаки, які визначені теоремою Касельса. Відмечено, що стандартна умова для MOV-атаки відповідає лише одній із умов теореми Касельса і не гарантує появу нециклічної структури групи точок. Запропоновано у майбутніх стандартах додати до тесту перевірку існування квадрату у порядку кривої.

Ключеві слова: еліптичні криві, криві Едвардса, порядок кривої, порядок точки, просте поле, розширене поле.

Бібліогр.: 9 найм.

UDC 681.3.06

On the incorrectness of a standard condition for MOV-attack to elliptic curves / A.V. Bessalov // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 238–239.

The analysis of two conditions of the Kassels theorem for bilinear pairing of points and for a MOV - attack is given. It is noticed that the standard condition for the MOV-attack corresponds only to one of the conditions of the Kassels theorem and does not guarantee the origin of a noncyclic structure of a group of points. It is offered to add to the MOV-test a quadrate presence one in a curve-order in the future standards.

Keywords: elliptic curves, Edwards curves, curve order, point order, prime field, extension field.

Ref.: 9 items.